UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AND ORDER: (1) AUTHORIZING THE USE OF A PEN REGISTER AND TRAP AND TRACE DEVICE; (2) AUTHORIZING RELEASE OF SUBSCRIBER AND OTHER INFORMATION; AND (3) AUTHORIZING THE DISCLOSURE OF LOCATION-BASED SERVICES	§	**Case No. A-10-561 M**

OPINION

This matter comes before the Court pursuant to a written and sworn application under 18 U.S.C. §§ 3122(a)(1), 3127(5), 2703(c)(1)(B) & (d) and FED. R. CRIM. P. 41 by an Attorney for the Government as defined by FED. R. CRIM. P. 1(b)(1)(B), and accompanying affidavit of a Drug Enforcement Administration Special Agent (hereafter, "Affiant"), applying for a multi-part order authorizing: (i) the installation and use of a pen register and trap and trace device; (ii) the disclosure of stored wire and electronic transactional records; and (iii) the disclosure of location-based data. On July 14, 2010, the Court authorized parts (i) and (ii) of the application, and took part (iii) of the application under advisement. This Order addresses that section of the application, requesting cell-site location information.[1]

I. GENERAL BACKGROUND

In general terms, federal law authorizes the use of four types of electronic surveillance as criminal investigative tools. The tools can be viewed on a graduating scale—as the intrusiveness

[1]The Application and previous order have been filed under seal. This opinion is not sealed because it has been carefully drafted to avoid discussion of confidential matters, and only addresses legal issues of general applicability to similar applications.

of each increases, the legal standard that the law enforcement agency must satisfy to use that tool increases accordingly. Pen registers[2] and trap and trace devices,[3] in most contexts the least invasive tools, require a law enforcement officer to certify that the information likely to be obtained by the pen register or trap and trace device "is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2). Stored communications and subscriber or customer account records require (generally speaking) "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (the "Stored Communications Act," or "SCA"). Search and seizure warrants are covered by FED. R. CRIM. P. 41 and its "probable cause" standard. Finally, wiretap orders have the highest legal standard, as they are governed by a detailed set of procedures laid out in 18 U.S.C. § 2501, *et. seq.* Wiretaps are often referred to as "super-warrants" because of the additional requirements beyond probable cause necessary for their issuance.

As technology has advanced, new investigative tools have become available that federal law does not explicitly address. The Court's focus in the present application is on cellular site location information ("CSLI"), which is information that resides on computer servers of telecommunications providers which allows law enforcement agencies to locate a cell phone, and its user, in both real time and, by accessing historical data, in the past. A request for CSLI presents a number of legal

---

[2]A "pen register" is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . ." 18 U.S.C. § 3127(3).

[3]A "trap and trace device" is "a device or process that captures the incoming electronic or other impulses which identify the originating number" or other identifiers "reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information not include the contents of any communication." 18 U.S.C. § 3127(4).

issues, and a growing number of decisions addressing these many have been handed down by magistrate and district judges in the past few years. The primary issue presented in those cases is the standard the Government's evidence must meet for it to obtain an order requiring the disclosure of CSLI, and whether that standard is different depending upon the type of information sought (historical v. prospective data), or the means by which the information is to be acquired (single tower, multiple towers, or GPS data).

After meetings in 2005-06 with members of the United States Attorney's office and representatives of law enforcement agencies, the magistrate judges in the Austin Division of this Court determined that a showing of probable cause would be required to obtain an order for any type of prospective CSLI. Those meetings were informal, and no written order expressing the basis for that conclusion was ever issued. In this opinion, the Court reviews the caselaw that has developed over the past five years on these issues, reviews the position of the Government, revisits the approach the Court has taken to date in these cases, and clarifies the procedures it will require when the Government wishes to obtain CSLI in the future.

II. THE CASES TO DATE

Beginning in 2005, magistrate and district judges began issuing published decisions addressing many of the questions raised by applications for CSLI. The first comprehensive opinion was issued by Magistrate Judge Stephen Wm. Smith of Houston. *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp.2d 747 (S.D. Tex. 2005) (hereinafter *Houston 2005 Order*).[4] In that decision, Judge Smith rejected what was termed the

[4]Because by their nature applications for CSLI have long, cumbersome titles, I will refer to the decisions in those cases in the following shorthand form: "*[CITY] [Year] Order*" followed by the citation to their reporting service (either the Federal Supplement or Westlaw).

government's "hybrid theory," by which it contended that CSLI was obtainable with less than probable cause through a hybridization of the authorities granted by the pen/trap statute and the Stored Communications Act ("SCA"). He concluded that CSLI required a showing of probable cause, as it was properly considered akin to a tracking device. Several courts followed with decisions reaching the same overall conclusion regarding probable cause. The first opinion to reach the opposite conclusion—that probable cause was not required for cell site information—came in December 2005 from Judge Gorenstein of the Southern District of New York. *New York 2005 Order*, 405 F. Supp.2d 435 (S.D.N.Y. 2005). Although Judge Gorenstein accepted the government's "hybrid theory," he made it clear that his decision was restricted to the facts before him, in which the government was only requesting "cell-site information concerning the physical location of the antenna towers associated with the beginning and termination of calls to and from" the subject phone. *Id*. at 437.

Magistrate and district judges across the country then began to weigh in on the issue.[5] To date, a strong majority have reached the same conclusion as Judge Smith.[6] Since Judge Gorenstein's opinion, several courts have followed his lead and distinguished between CSLI obtained from a single cell tower and CSLI obtained from multiple towers or with GPS technology. In these courts'

---

[5]Judge Smith's recent testimony to the Congress on these issues contains the most comprehensive gathering of the CSLI cases to date. *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Comm. on the Judiciary and Subcomm. on the Constitution, Civil Rights, and Civil Liberties*, 111th Cong. Exh. B (2010) (statement of Stephen Wm. Smith, United States Magistrate Judge), available electronically at http://judiciary.house.gov/hearings/pdf/Smith100624.pdf (last viewed July 28, 2010).

[6]*See* Adam Koppel, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. Miami L. Rev. 1061, 1081 n.160 (2010) (collecting cases).

view, making this distinction was warranted because triangulation (via information from multiple towers) and GPS provide more precise location capabilities, and thus CSLI from these sources is more invasive. The majority approach, however, has been to require the same "probable cause" showing for CSLI regardless of the means by which the information is to be acquired. Significantly, although a minority of decisions have allowed limited CSLI with only a showing of "specific and articulable facts,"[7] there are no published decisions permitting multiple tower or GPS-based CSLI without a showing of "probable cause."[8]

Another distinction has been made between CSLI that allows law enforcement agencies to locate the target phone user in real time and CSLI records of phone locations in the past. Only a few courts have directly addressed the issue of historical CSLI. Most courts have assumed (with little or no discussion) that historical CSLI may be obtained under the SCA because it only amounts to stored records. In a detailed analysis of the issue, the *Pittsburgh 2008 Order* concluded that historical CSLI is indistinguishable, from a Fourth Amendment and statutory perspective, from prospective CSLI and that probable cause is required for historical records as well. 534 F. Supp.2d at 585. This decision is on appeal to the Third Circuit.

III. THE GOVERNMENT'S POSITION

In the case at hand, the Government has asked for the entire spectrum of CSLI, as opposed to the more limited requests that have been made in some of the prior cases. While it presents

---

[7]For example, *see New York 2006 Order*, 460 F. Supp.2d 448, 461 (S.D.N.Y. 2006) (Kaplan) (authorizing the disclosure of prospective cell site information only where the government does not seek triangulation information or location information other than that transmitted at the beginning and end of particular calls).

[8]*See Pittsburgh 2008 Order*, 534 F. Supp. 2d 585, 599-600 (W.D. Pa. 2008) (collecting cases).

evidence in the form of an affidavit to demonstrate probable cause to support the application, the Government does not concede that probable cause is legally required for this type of CSLI, and instead alternatively offers a condensed version of the "hybrid theory" argument discussed above. *See* Application, n.10.

The more complete version of the hybrid argument has been expressed in many places, but perhaps is best expressed in Judge Gorenstein's December 2005 Order. In short, the hybrid theory contends that statutory authority to obtain CSLI on something less than probable cause can be implied from provisions in three statutes. The argument starts with a provision in the Communications Assistance to Law Enforcement Act ("CALEA"), which states that "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a)(2)(B). This provision thus prohibits an order granting pen register and trap and trace authority from also permitting location-based information. The argument notes, however, that use of the term "solely" in CALEA can be read to suggest that if the information is obtained pursuant to the pen/trap statute *plus* some other statute, then location-based information may be included. The government employs the SCA as this second authority, and contends that an order granted pursuant to the SCA, combined with the pen/trap authority, permits the release of CSLI upon the government meeting the SCA standard of "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). In sum, the government views a pen/trap order as a necessary but insufficient condition for compulsory disclosure of CSLI. Once the pen/trap order is combined

with an order pursuant to the SCA, the argument goes, the "hybrid theory" allows for the disclosure of CSLI without having to establish probable cause.

Numerous cases have already exhaustively reviewed the Government's hybrid argument, and there is no need to restate the various failings courts have found with it. *See, e.g. Houston Order 2005*, 396 F. Supp 2d at 761-765; *Puerto Rico Order 2007*, 497 F.Supp. 2d 301, 306-311 (D. Puerto Rico 2007). The need to analyze the argument is made even less important given that the United States Attorney's office in this division has chosen not to pursue the hybrid argument in its applications for CSLI, but rather has instead included with applications seeking such data affidavits purporting to establish probable cause to support its receipt.[9] Having said this, for the reasons set out in the many cases that have already rejected the argument, the undersigned agrees that the Government's hybrid theory cannot support the issuance of an order granting the Government access to CSLI.[10]

IV. CELL PHONES AS TRACKING DEVICES

The question thus becomes, what is the authority for granting the Government access to CSLI, if it cannot be found within these statutes? In short, the answer would seem to be the Fourth Amendment, in conjunction with FED. R. CRIM. P. 41. The general rule regarding warrants is well

[9]The standard application for CSLI used by the U.S. Attorney's office contains one or more footnotes in which the Government states that it does not concede that probable cause is required to obtain CSLI, and that it offers such evidence without waiving its right to contend in this or other forums that a lesser standard is appropriate.

[10]The most obvious reason why the hybrid theory fails is that the SCA limits its application to "electronic communications," and specifically states that information from tracking devices is not an "electronic communication." 18 U.S.C. § 2510(12)(C). As is discussed below, CSLI is rather obviously information from a "tracking device" as that term is defined by federal law. There are many more subtleties to the problems with the hybrid argument, but because those have been well catalogued in the earlier opinions, they will not be repeated here.

known. The government may not conduct a search or seizure without a warrant, unless one of a very few specifically established and well-delineated exceptions applies.[11] *Katz. United States*, 389 U.S. 347, 357 (1967). In determining whether a "search" will occur through an investigative technique, courts look to whether the investigation would intrude on a subjective expectation of privacy that is also objectively reasonable. *Id.* at 361. Several of the courts to examine the CSLI issues have concluded that use of CSLI to track the movements of individuals is a "search" under the Fourth Amendment. *See, e.g., Houston Order 2005*, 396 F. Supp.2d at 756-57; *Pittsburgh Order 2008*, 534 F. Supp.2d at 611-616. As noted in the *Pittsburgh Order*,

> Americans do not generally know that a record of their whereabouts is being created whenever they travel about with their cell phones, or that such record is likely maintained by their cell phone providers and is potentially subject to review by interested Government officials. And second . . . most Americans would be appalled by the notion that the Government could obtain such a record without at least a neutral, judicial determination of probable cause.

Id. at 611. When it adopted the E-911 legislation, Congress itself recognized the expectation of privacy that cell phone users have in their location information, when it expressly stated in the legislation that a customer "shall not be considered to have approved the use or disclosure of or access to . . . call location information concerning the user of a commercial mobile service. . . ." *See* 47 U.S.C. § 222(f). As Judge Smith noted, this provision makes CSLI

> a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer. Based on this statute, a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.

Houston Order 2005, 396 F. Supp.2d at 757.

---

[11]The government does not contend that any exception to the warrant requirement applies here, although, as noted in the previous footnote, it also does not concede that it must demonstrate probable cause to obtain this information.

Moreover, when presented with whether use of investigatory techniques that do not fit easily within the statutorily or constitutionally-authorized tools constitute "searches" under the Fourth Amendment, the Supreme Court has fallen back to these same basic principles. For example, in a recent case involving the use of a thermal imaging device, the Supreme Court concluded that when the government uses a device not in general public use to "explore details of the home that would previously not have been knowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

Similar concepts have been adopted with regard to the use of tracking devices. Historically, there has been very little guidance available in either statutes or case law regarding the procedure and standards applicable to the use of tracking devices. Prior to recent amendments to the Federal Rules of Criminal Procedure, the most detail available regarding the use of tracking devices was found in a statute more notable for what it did *not* state than what it did. That entire statute reads:

> (a) **In General.**— If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.
>
> (b) **Definition.**— As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

18 U.S.C. § 3117. In the two seminal cases addressing tracking devices, the Supreme Court concluded that the question of whether use of a tracking device requires a warrant turns on whether the device will track the person or object only in public places, or will also extend to places in which there is a legitimate expectation of privacy. *See United States v. Knotts*, 460 U.S. 276, 284-85 (1983) (legality of monitoring beeper depends on Fourth Amendment legitimate expectation of

privacy standard); *United States v. Karo*, 468 U.S. 705, 714 (holding Fourth Amendment was violated when agents used beeper to locate object within a home). In *Karo* the Court declined to decide whether a search warrant to use a beeper required demonstration of probable cause, or the lesser standard of "reasonable suspicion." *Id.* at 718 n.5. The Courts of Appeals that have addressed this issue have held, however, that probable cause is the appropriate standard when such devices track people or objects into non-public locations. *See e.g., United States v. Mixon*, 977 F.2d 921, 923 (5th Cir. 1992) (upholding use of transponder in plane on demonstration of drug courier activity sufficient to constitute probable cause).[12] In adopting Rule 41(f)(2) in 2006, the Supreme Court (with Congress' tacit approval[13]) brought tracking devices into Rule 41. The new rule explicitly adopted the definition of "tracking device" contained within § 3117. FED. R. CRIM. P. 41(a)(2)(E). The amendments did not, however, resolve the question of the appropriate standard of review for judicial officers presented with tracking device warrants. As the Advisory Committee noted in its comment,

> The tracking device statute, 18 U.S.C. § 3117, does not specify the standard an applicant must meet to install a tracking device. The Supreme Court has acknowledged that the standard for installation of a tracking device is unresolved, and has reserved ruling on the issue until it is squarely presented by the facts of a case. *See United States v. Karo*, 468 U.S. 705, 718 n.5 (1984). The amendment to Rule 41 does not resolve this issue or hold that such warrants may issue only on a showing of probable cause. Instead, it simply provides that if probable cause is shown, the magistrate judge must issue the warrant. And the warrant is only needed

---

[12] *See also United States v. Cooper*, 682 F.2d 114, 115-16 (6th Cir. 1982); *United States v. Ellery*, 678 F.2d 674, 677-78 (7th Cir. 1982); *United States v. Little*, 735 F.2d 1049, 1054-56 (8th Cir. 1984).

[13] Any rule of procedure is prepared by advisory committees and submitted to the Judicial Conference, which then transmits the rule, as approved or revised, to the Supreme Court for review. If approved by the Supreme Court, the rule is then transmitted to Congress, and becomes effective unless specifically rejected by the Congress. *See* 28 U.S.C. §§ 2071-74.

> if the device is installed . . . or monitored . . . in an area in which the person being monitored has a reasonable expectation of privacy.

FED. R. CRIM. P. 41, comment to 2006 amendments, at subdivision (d).

Many of the cases to review applications for CSLI have held, or at least strongly suggested, that a request to use a cell phone to track the movements of a person fits squarely within the definition of a "tracking device." *See, e.g., Houston Order 2005*, 396 F. Supp.2d at 753-757; *Baltimore Order 2005*, 402 F. Supp.2d 597, 603-605 (D. Md. 2005); *Milwaukee Order 2006*, 2006 WL 2871743 (E.D. Wis. 2006); *New York Order 2009*, 2009 WL 159187 (S.D.N.Y. 2009). Frankly, it is difficult—if not impossible—to reach any other conclusion. As Judge Smith noted when he first looked at this issue in 2005,

> the definition [of tracking device] is striking for its breadth. Note that a device is covered even though it may not have been intended or designed to track movement; it is enough if the device merely ''permits'' tracking. Nor does the definition suggest that a covered device can have no function other than tracking movement. Finally, there is no specification of how precise the tracking must be.

Houston Order 2006, 396 F. Supp.2d at 753. The definition contained in § 3117, and incorporated into FED. R. CRIM. P. 41, compels the conclusion that a cell phone is a tracking device when it is used to locate a person and track their movements.

As noted, in its application, the Government suggests that an application that requests only single tower information may be granted under the pen/trap statute and/or the SCA on a showing of less than probable cause, on the theory that such data does not amount to tracking information, because it cannot precisely locate the phone user, but rather only provides information regarding the location of the phone provider's cell tower. The Government states:

> That the disclosure of a cell site number and that cell-site's physical tower location constitutes disclosure of a subscriber's "physical location" is doubtful. Rather, cell-

> site data discloses only the physical location of a fixed antenna tower that belongs not to the *subscriber*, but to a third party telecommunications provider. And to allay any concern about the "private" nature of that tower's location[,] cell site towers are always visually observable from the "public highway."

See Application at 8-9 n.10 (emphasis in original). But this argument is a bit disingenuous, at least insofar as it suggests that the Government is only interested in knowing where cell towers are. If this were true, the Government would not be applying for the orders it is requesting. Clearly, the Government's interest in the cell towers is based upon its desire to know where the subject of its investigation is *in relation to* particular cell towers. *That* information is not something in the public domain. More to the point, the Government's argument—because information from a single tower does not provide precise location data, collecting this type of information is not tracking data—contravenes the statutory definition of a tracking device, and the case law that has developed around use of such devices.

As Judge Smith noted, nothing in the statutory definition requires that a "tracking device" provide exact or precise location information. Indeed, the case law that developed around the use of such devices suggests just the opposite. When tacking devices were first being discussed in case law, law enforcement was using "transponders" and "beepers" which were tracked with receivers that permitted agents to have only general information regarding the location of the tracked object or person. The level of information obtained from tracking devices was thus akin to (and indeed, less precise than) what law enforcement agents today can know about a modern cell phone user's location from information from a single cell tower. *See, e.g. United States v. Levine*, 80 F.3d 129, 132-133 (5th Cir. 1996) (discussing a transponder used to track currency stolen in a bank robbery, describing the tracking unit as containing lights and audio signals to indicate proximity and direction

of transmitter).[14] Despite the lack of precision provided by "traditional" tracking devices, courts have uniformly applied a probable cause standard for the Government to obtain permission to use such devices when those devices might track an object beyond public places. *See Mixon*, 977 F.2d at 923, and cases cited *supra* at p.10. There is no reason to believe, therefore, that the Government should have a lesser burden to obtain "single tower" information than it had (and still has) to obtain the functionally identical information from a transponder or beeper.[15] Again, the very reason the Government wishes to obtain CSLI—whether it is single tower, multiple tower, or GPS data—is to receive information about the location of the cell phone user, whether that be to place the suspect in a city, on a particular block within a city, or at a particular table inside a house. Although each of these represents a different level of precision, they all represent information provided from a "device which permits the tracking of the movement of a person or object." By law, that makes the device a "tracking device." 18 U.S.C. § 3117(b).

---

[14]*See also United States v. Berry*, 300 F. Supp. 2d 366, 368 (D. Md. 2004) ("Measured against today's technology, a beeper is unsophisticated, and merely emits an electronic signal that the police can monitor with a receiver. The police can determine whether they are gaining on a suspect because the strength of the signal increases as the distance between the beeper and the receiver closes.")

[15]It is for this reason that I find the cases adopting a lesser standard for "single tower" CSLI unpersuasive. Similar problems befall orders that distinguish—and grant on less than probable cause—applications that only ask for CSLI at limited times, for example when calls are initiated and terminated. *See e.g.., Houston 2007 Order*, 622 F. Supp.2d 411 (S.D. Tex. 2007) (Rosenthal). If an intrusion into a legitimate expectation of privacy takes place only once, or in limited bursts, it is still an intrusion, and it still requires probable cause under the Fourth Amendment. Put another way, if the information is used to track a person's movements, even on a limited basis, it is still a tracking device. And there is nothing in any of the relevant statutes that makes a distinction between "limited" location information and fully robust, minute-by-minute location information. If the hybrid argument works for the former, it must work for the latter as well. Thus, the distinctions found by these courts seem more about trying pragmatically to find a middle route than being totally faithful to the statutory language.

Moreover, the Government's argument ignores other realities. First, notwithstanding what has become a "boilerplate" footnote in all of the Government's applications suggesting that it is only seeking to know the location cell towers, the application here requests far more than single tower data. Specifically, it asks for:

> location-based data that will assist law enforcement in determining *the exact location of the Target Devices* (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the third party Provider's infrastructure). This request for location-based data includes the request for an order directing Providers to employ and to disclose the results (through any means reasonably available) of any all available location-based services, including but not limited to real time cell-site data and those "Enhanced-911" services developed by the Providers to comply with the provisions of 47 C.F.R. § 20.18.

Application at 8-9 (emphasis added). Thus, whatever arguments might exist regarding distinctions between the varying levels of CSLI leading to differing standards—arguments that I find unpersuasive as already noted—those arguments have nothing to do with the present application.

Finally, cell phone technology is moving quickly to the point where debates about single tower vs. multiple tower triangulation are academic. Estimates from three years ago were that over 90% of cell phones then in use had GPS capabilities, through which the target phone could be located to within as little as 50 feet.[16] The Federal Communications Commission and its Enhanced 911 initiative requires cell phone carriers to be able to pinpoint the location of their customers in case of an emergency call.[17] And although the main motivation behind the 911 initiative has been public

---

[16]*See* Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 Hastings Comm. & Ent L.J. 421, 427 (2007).

[17]These rules apply to all wireless licensees, broadband Personal Communications Service licensees, and certain Specialized Mobile Radio licensees. The E-911 program had two parts. Under Phase I, the FCC required carriers, within six months of a valid request by a local Public Safety Answering Point (PSAP), to provide the PSAP with the telephone number of the originator of a wireless 911 call and the location of the cell site or base station transmitting the call. In Phase II, the

safety, it is not surprising that companies are now trying to turn those required investments into commercial opportunities by offering non-emergency tracking for a monthly fee. For example, by paying a monthly fee and subscribing to MobileMe, an iPhone user can determine exactly where his or her phone is (a very handy "app" when a user misplaces their phone). The bottom line is that cell phones undoubtedly have become "electronic . . . device[s] which permit[ ] the tracking of the movement of a person or object." 18 U.S.C. § 3117. They *are* tracking devices.[18]

V. TRACKING DEVICE PROCEDURE AND DEMONSTRATING PROBABLE CAUSE

What is the significance of the conclusion that a cell phone acts as a tracking device when it transmits information about its location? The significance is that if cell phones squarely meet the definition of "tracking devices" it is time to stop treating them as something else, at least when the Government seeks to use them to track a person's movements. Rule 41 contains express procedures governing tracking device warrants, and those procedures need to be followed with regard to future requests for CSLI. This means several things. First, in past applications, the Government has taken the position that it has no obligation to provide notice of the tracking to the cell phone user, as its

---

FCC requires wireless carriers, within six months of a valid request by a PSAP, to begin providing information that is more precise to PSAPs, specifically, the latitude and longitude of the caller. This information must meet FCC accuracy standards, generally to within 50 to 300 meters, and requires the development of new technologies and upgrades to local 911 PSAPs.

[18]That a cell phone is a tracking device for these purposes does *not* mean that it is only a tracking device. As any user of a "smart phone" knows, the devices have many uses. From the standpoint of law enforcement, this means that the phone may be a tracking device for some purposes, act as a pen register for others, and be identical to a "land-line" phone—and thus subject to a Title III wiretap—for yet other purposes. Accordingly, concerns expressed by some that finding a cell phone to be a tracking device creates a "slippery slope" that will lead to unintended consequences are misguided. Judge Smith addressed this very issue in his *Houston 2005 Order* in some detail, and demonstrates clearly that the concerns are without basis. 396 F. Supp.2d at 755-56.

notice obligation was met by service of the order on the telecommunications provider from whom it received the CSLI. This does not meet the requirements of Rule 41, which provides that when a tracking device warrant is authorized, "the officer must serve a copy of the warrant on the person who was tracked or whose property was tracked." FED. R. CRIM. P. 41(f)(2)(C).[19] Thus, warrants seeking CSLI must meet this obligation of Rule 41. Similarly, a return must be filed, as with all other warrants. FED. R. CRIM. P. 41(f)(2)(B).

Applying Rule 41 to CSLI requests also raises the issue of what precisely is meant by the requirement of probable cause in this context. Surprisingly, this is an issue that has been little discussed in the many recent opinions regarding CSLI. Perhaps this is so because it is a complex question, with many subtleties, and perhaps also because the labyrinth created by a patchwork of electronic surveillance statutes and the government's hybrid argument have dominated the discussion to date. Regardless, the probable cause issue is deserving of analysis.

In many applications, including the present one, the evidence submitted in the probable cause affidavit follows a similar pattern: (1) there is evidence that the user of the target phone is dealing in narcotics; (2) there is evidence that the target phone is used in the narcotics dealing; and (3) being able to track the user's movements would assist in the investigation (for example, by helping to identify associates, stash houses, or sources of supply). On its face, this may seem adequate to support the issuance of a warrant for CSLI. On closer inspection, however, this conclusion is not so clear. Indeed, some judges presented with this very sort of information have declined to issue warrants for CSLI on the ground that it fails to demonstrate probable cause to believe that the CSLI would result in *evidence of a crime*—the Rule 41 requirement—but rather demonstrates something

[19]The Rule expressly permits delayed notice with the court's approval.

less than that, roughly akin to probable cause to believe that it would result in *evidence that would be relevant to the case*. *See, e.g. Washington Order 2006*, 407 F. Supp.2d 134 (D.D.C 2006).

This conclusion by Judge Facciola is based on his view that Rule 41 only permits tracking warrants to be issued for the categories laid out in Rule 41(c), which are: "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained." FED. R. CRIM. P. 41(c). While I agree with much of Judge Facciola's well-reasoned opinion, I believe his view of the "probable cause" question may read more into Rule 41 than was intended. First, it is important to remember that tracking devices were only added into Rule 41 in 2006, and the list contained in Rule 41(c) pre-dates that amendment. When Rule 41 was amended in 2006, distinctions were carefully drawn between a warrant to search for or seize a person or property, and a warrant for a tracking device. For example, in Rule 41(b), which sets out a list of the warrants a judge has authority to issue, tracking devices are separately listed, distinct from, and in addition to, person and property warrants. Rule 41(d) identifies two types of warrants that may be issued: a warrant "to search for or seize a person or property," and a warrant "to install a tracking device." The pattern is repeated in Rule 41(e), which addresses issuing a warrant, and Rule 41(f), governing the execution and return of warrants, where in each there are entirely different subsections for person or property warrants than for tracking warrants. The manner in which the 2006 amendments to Rule 41 were drafted strongly suggests a warrant for a person or property was viewed as a different animal from a warrant for a tracking device. Given this, and given that the list of things for which a warrant could be issued pre-dated the 2006 amendments, a fair conclusion could be that the list contained within Rule 41(c) is a list of the things for which a search or seizure

warrant for a person or property may issue, and is not intended to similarly constrict tracking device warrants.

Even if the narrower reading Judge Facciola gives Rule 41(c) is accepted, there is an interpretation of the rule which is nonetheless more generous than the conclusion he reaches. For example, in the very case before him, he describes the evidence as being that the target "used the cell phones at issue to conduct his drug business." 470 F. Supp.2d at 135. Thus, even assuming that the government was required to fit its tracking device into the list contained in Rule 41(c), issuing a tracking device for the phone would seem to fit within Rule 41(c)(3), which permits a warrant for "property designed for use, intended for use, or used in committing a crime." The phone was being "used in committing a crime," and a tracking device for that phone is a tracking device for an item listed in Rule 41(c). Similarly, a request for a CSLI warrant for a fugitive's cell phone would seem to fit within 41(c)(4), which authorizes a warrant for "a person to be arrested." In that case, the warrant would be for a tracking device for "a person to be arrested." As noted in the preceding paragraph, I have doubts that Rule 41(c) was intended to be read in this manner, but even if read this way, the Rule can nonetheless support the issuance of tracking devices.

This is not to say that Judge Facciola's concerns are totally unwarranted, as there is a legitimate scope problem with using a cell phone as a tracking device. The probable cause affidavit for CSLI rarely suggests that every activity in the target's life is illegal activity, yet receipt of CSLI will permit the government to "follow" the phone user's movements 24 hours a day, 7 days a week, wherever they go, whatever they are doing. When presented with the similar scope issue created by a wiretap (where agents have the functional ability to listen in on all phone calls from the tapped phone, regardless of their subject matter), Congress imposed statutory limits, requiring agents to

terminate their eavesdropping when the calls do not concern the subject matter of the investigation. 18 U.S.C. § 2518(5).[20] Because there are no statutes dealing with CSLI, this creates a problem of scope for an authorizing judge. Does authorizing the Government to surreptitiously "follow" a person's every movement by use of their cell phone for 45 days, with no order or rules limiting where they "follow" the person, comport with the Fourth Amendment? The Supreme Court noted in *Coolidge v. New Hampshire* that the particularity requirement of the Fourth Amendment is intended to protect against "general exploratory rummaging in a person's belongings." 403 U.S. 443, 467 (1971) (plurality opinion). Would the unlimited ability to track a person's movements amount to allowing a "general exploratory rummaging" in their lives? On the flip side of these concerns, it is clear that tracking warrants may issue, and the highest standard that any court has suggested is appropriately applied to tracking devices is "probable cause." So where is the appropriate place to draw this line?

One place to look for guidance is within the cases that have reviewed the issuance of tracking devices. In *United States v. Mixon*, the Fifth Circuit rejected the defendant's argument on appeal that the evidence gathered through use of a tracking device on a private plane to "trace its travel" should have been excluded. 977 F.2d at 922. The court summarized the evidence to support the issuance of the warrant for use of the device as follows:

> The government was first alerted to the modification of the plane [to increase its fuel capacity, and therefore its range] by a confidential source. Agent Luzak duly corroborated the information. Government agents personally observed the rear seat

[20]The relevant language states that "[e]very order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."

> being removed and the extra tanks added to the wings. A check on the individuals involved uncovered a convicted drug felon, Magee. A check on Matrone revealed that he was also a criminal with a history of forgery arrests and a conviction on aiding and abetting wire fraud. A check on the registered owner of the pickup truck, Alex Vega, revealed that he had violated firearm regulations. The modified plane fit the profile of a drug smuggling aircraft. All of the information together was more than enough to give the agents probable cause to suspect the individuals of planning to smuggle drugs and it was proper to request a warrant to place a transponder to trace the Cessna in question.

Mixon, 977 F.2d at 923 (citing *Illinois v. Gates*, 462 U.S. 213 (1983)). Thus, the agents had reason to suspect the plane was being used to import drugs, they had no way to follow it, and the use of the transponder allowed them to identify when the plane arrived in the United States "from the direction of Jamaica." The courts in *United States v. Ellery* and *United States v. Cooper* reached similar conclusions, approving warrants that authorized the installation of tracking devices on a parcel carrying a chemical, and a UPS package, respectively, on evidence demonstrating that there was probable cause to believe that the chemical was headed to a drug lab, and that the package was likely to be stolen by a UPS employee. *Ellery*, 678 F.2d 674; *Cooper*, 682 F.2d 114. In *United States v. Harmon*, the Eighth Circuit suppressed evidence obtained from a transponder on a plane, on the grounds that the warrant affidavit failed to include evidence of the reliability of the informants quoted in the affidavit, and failed to offer any corroboration of the informant's evidence. Some common threads among these four opinions are: (1) the review of the probable cause evidence was exacting in each, and (2) the approved devices provided far less intrusive information than CSLI will provide (indeed, in the *Ellery* case the warrant permitted the monitoring of the beeper for "not more than 72 hours, after which a report was to be made to the issuing Magistrate," 678 F.2d at 115).

In sum, there are difficult questions presented by the probable cause determination on CSLI applications, and it is not obvious what the answers to those questions are (at least it is not obvious

to me what the answers are). Accordingly, until there is more guidance from Congress and the courts on these issues, I will take a cautious approach toward CSLI requests. First, I will insist on strict adherence to the requirements of Rule 41 on all requests for CSLI, including requests for historical data.[21] The warrants will be granted only on a showing of probable cause, may only last 45 days (in the case of prospective warrants), and notice on the person tracked is required (although it may be delayed). The warrants must be returned to the magistrate judge identified on the warrant. I will further require that warrants for CSLI be "stand alone" documents, and not be included as part of an application for a pen register, trap and trace, or subscriber records. With regard to probable cause, I will not take as narrow an approach as Judge Facciola's and insist that the CSLI must itself qualify as "evidence of a crime." But the warrant affidavit must demonstrate that there is probable cause to believe that tracking the phone will *lead* to evidence of a crime. One example of evidence that would meet this standard is evidence that the phone to be tracked is intimately involved in the crime being investigated; for example, where the sole or dominant purpose of the target phone is its use in a drug trafficking organization to make and receive calls related to the drug business. Evidence that a person has a cell phone and is engaged in criminal conduct is not enough to meet this standard. In investigations, being granted a warrant for CSLI should be the exception, not the rule, and if all the Government must prove to receive CSLI is that the target has a cell phone and probably engages in crime, then a CSLI warrant would be issued in *every* criminal investigation. As a result, I will

[21] I recognize that many courts have distinguished between prospective and historical CSLI and have granted requests for historical CSLI under the SCA on a showing less than probable cause. In light of the *Pittsburgh 2008 Order* (which makes a persuasive case for a probable cause standard for this data), and its pendency on appeal to the Third Circuit, out of an abundance of caution I believe it is prudent to require probable cause for historical data until we receive an opinion from the Third Circuit on that issue. Once that order is handed down, I will revisit the issue of historical CSLI.

require that there be more than this contained within the Government's application.[22] What this will be is necessarily a fact-intensive question, and all that can be provided at this point are the general guidelines just discussed. In other words, we will have to make law on this issue the old-fashioned way, case by case.

In the present case, the Government has submitted an affidavit from the case agent in this investigation indicating that the target phone user:

> and his associates regularly travel to other locations in order to conduct their criminal activities. . . . Location-based services would assist law enforcement to know when [the target] is traveling in [a specific city] are to conduct narcotics trafficking activities. There is probable cause to believe that location-based services would help yield relevant evidence in this case regarding the identity of coconspirators and the timing and frequency of drug transactions. Even if law enforcement had the manpower to maintain 24-hour surveillance on [the target], such constant surveillance would alert [him or her] to the presence of law enforcement. Location-based services would allow law enforcement to maintain a lower profile in order to maximize the chances of obtaining evidence against [the target].

Affidavit in support of Application at ¶ 3(f). The affidavit also states that the target has at least two cell phones, and has used them related to his criminal endeavors. There is no evidence presented regarding the frequency with which each of the target phones is used as part of the criminal conduct. Reviewing this evidence under the principles just discussed, it does not "make the grade" in demonstrating probable cause to believe that tracking these phones would result in the discovery of evidence of a crime. Indeed, the agent states directly that it would do something less—"help yield relevant evidence in this case."

---

[22]In a case in which the Government is seeking CSLI to track a person so that an arrest warrant may be executed, it will be sufficient if the warrant affidavit demonstrates the existence of the warrant, and probable cause to believe that the target phone is in the possession of the fugitive.

Accordingly, on the present affidavit, with the facts now presented, the request for an order or warrant for CSLI will be DENIED without prejudice to being resubmitted with additional evidence sufficient to meet the standard discussed herein.

SIGNED this 29th day of July, 2010.

ANDREW W. AUSTIN
UNITED STATES MAGISTRATE JUDGE